Before the
Federal Communications Commission
Washington, D.C.

In the Matter of	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	WC Docket No. 18-89

COMMENTS OF THE
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)[1]

CCIA respectfully submits these Comments in the above-referenced proceeding[2] in response to the Wireline Competition Bureau's Public Notice seeking comment on "the applicability of provisions in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (*2019 NDAA*) to the [. . . NPRM] and to the programs the Commission oversees."[3] CCIA appreciates the Commission's interest in protecting communications networks in the U.S. and addressing potential vulnerabilities in light of the changes presented by the NDAA. CCIA maintains that the Commission should develop a clearer and more focused policy that addresses real harms while also limiting uncertainty and compliance burdens for Universal Service Fund (USF) recipients. In addition, the Commission, in coordination with other agencies, like the Department of Homeland Security (DHS), should conduct a wider effort to understand the extent to which there are problems or vulnerabilities on networks in the U.S., and the extent to which

[1] CCIA represents large, medium, and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications, and Internet products and services. Our members employ more than 750,000 workers and generate annual revenues in excess of $540 billion. A list of CCIA's members is available online at http://www.ccianet.org/members.

[2] *Protecting against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, *Notice of Proposed Rulemaking*, (Apr. 17, 2018).

[3] *Wireline Competition Bureau Seeks Comment on Section 889 of John S. McCain National Defense Authorization Act for Fiscal Year 2019*, WC Docket No. 18-89, *Public Notic*e, (rel. Oct. 26, 2018).

they derive from components and technologies produced by companies like China's Huawei and ZTE. To the extent the Commission is called upon to make judgments regarding national security, it should defer to the expert U.S. Government agencies.

In this Public Notice, the Commission seeks comment on NDAA Section 889(b)'s relevance to the NPRM, and particularly whether it supports the prohibitions that the Commission seeks to apply with respect to entities' use of USF or other funding programs to support purchases of covered telecoms equipment or services. It is important for the Commission to recognize that Congress wrote Sec. 889 not as a blanket and absolute restriction on any use of covered equipment, but with exceptions. In particular, Congress sought to limit the prohibitions on procuring or obtaining "covered telecommunications equipment or services" by saying that they must be "a substantial or essential component" or a "critical technology".[4] This means that if the provider has covered telecommunications equipment in a portion of its network, but that portion of the network would not be used in the provision of services to the executive agency, then the prohibitions in Sec. 889 should not apply. Moreover, if covered equipment is not a substantial or essential component in a provider's network used to provide services to an executive agency, then the prohibitions in Sec. 889 should not apply. This confinement to substantial or essential components or critical technology also extends to subsection (b) of Sec. 889, for (b) refers to "the equipment, services, or systems described in subsection (a)".[5] Indeed, the Commission must recognize that Sec. 889's prohibition is limited to "covered equipment" that is a "substantial or essential component" or a "critical technology" of a system related to a federal contract. Furthermore, in relation to this USF proceeding, Sec.

[4] NDAA Sec. 899(a)(A) & (B).
[5] NDAA Sec. 899(b).

889 should not be read to bar entities that have used "covered equipment" in other, non-USF settings.

The Commission should also recognize that Congress provided further limitations that also apply to agencies administering loan, grant, or subsidy programs, including the Commission itself. Sec. 889(a) does not prohibit procurements with entities that provide "a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements",[6] nor should it be construed to "cover telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles."[7] Those limitations appear verbatim in Sec. 889(b)(3), showing that Congress intended to provide the same exceptions to agencies administering loan, grant, or subsidy programs. In particular, the exception contained in (b)(3)(A) allows executive agencies to procure services from an entity if the service provided by the entity connects to the facilities of a third party for services such as backhaul, roaming or interconnection. Similarly, the exception in (b)(3)(B) does not restrict grants for procurement from or contracting with providers whose systems may have covered equipment as a substantial or essential component if the equipment in question cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles. These exceptions are especially important for USF programs because they account for the difficulty in determining where threats could be on a network.[8] Congress specifically repeated the exceptions from (a)(2) as (b)(3) to ensure that networks connecting to facilities or

[6] NDAA Sec. 899(a)(2)(A).
[7] NDAA Sec. 899(a)(2)(B).
[8] *See* CCIA Comments at 4-5, WC Docket No. 18-89 (June 1, 2018) (quoting relevant testimony from Dr. Charles Clancy, Professor of Electrical and Computer Engineering at Virginia Tech, before the House Energy and Commerce Committee).

interconnecting with networks that may have "covered equipment" would not suffer from the prohibitions in (a) and, more importantly for this proceeding, (b).

The Commission should take particular notice of the exception in (b)(3)(B), which excepts "equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles." This exception attempts to account for where equipment could be on a network and the kind of visibility it could allow, *e.g.*, certain networking layers. The Commission should consider whether routing and/or redirection could occur with or without the knowledge of the entity with "covered equipment" in its network or an entity interconnecting with a network that has "covered equipment".

The limitations and exceptions outlined above, in particular those in Sec. 889(b)(3), should be particularly instructive to the Commission in this proceeding because they relate to the practicality and administrability of what is proposed in the NPRM. As stated in CCIA's initial Comments, though "the U.S. market shares of Huawei and ZTE are relatively small compared to the rest of the world", their equipment is pervasive worldwide.[9] Indeed, the limitations and exceptions in Sec. 889 seem to account for this fact as well as the difficulties that U.S. executive agencies and their personnel would face in obtaining connectivity and communications capabilities in African, Asian, European, and/or Latin American countries where the NDAA's "covered equipment" are far more prevalent.[10] Without the limitations and exceptions, it would be exceedingly difficult for U.S personnel abroad to comply with an outright ban.

CCIA appreciates the Commission's attention to this issue, and encourages the Commission to develop a clearer, focused policy that addresses real harms; limit uncertainty and compliance burdens for USF recipients; and coordinate with other agencies, like DHS, on a

[9] *Id*. at 2.

[10] Justina Crabtree, *'China is everywhere' in Africa's rising technology industry*, CNBC (July 28, 2017), https://www.cnbc.com/2017/07/28/china-is-everywhere-in-africas-rising-technology-industry.html.

wider effort to understand the extent to which there are problems or vulnerabilities on networks in the United States.

November 16, 2018

Respectfully submitted,

/s/ John A. Howes, Jr.
Policy Counsel
Computer & Communications Industry Association (CCIA)
655 15th Street, NW Suite 410
Washington, D.C. 20005
(202) 783-0070
jhowes@ccianet.org